IJCLC

Indonesian Journal of Criminal Law and Criminology (IJCLC)
Volume 5, Issue 3, November 2024, 104-116

E-ISSN: 2745-7184
P-ISSN: 2745-7192

Pusat Kajian Hukum Pidana dan Kriminologi
Fakultas Hukum, Universitas Muhammadiyah Yogyakarta
E-mail: ijclc@umy.ac.id

Perlindungan Hukum Korban Terhadap Pelanggaran Hak Privasi Dalam Pembuatan Konten Menggunakan *Drone*

Akmal Zulham Nurkamal, Laras Astuti
Program Studi Hukum, Fakultas Hukum, Universitas Muhammadiyah Yogyakarta
Email : larasastuti@law.umy.ac.id

Submitted: 18-07-2024; Reviewed: 02-08-2024; Revised:07-11-2024; Accepted: 24-11-2024
DOI: https://doi.org/10.18196/ijclc.v5i3.23254

Abstrak

Selama drone menjadi sesuatu yang baru, masyarakat selalu khawatir tentang bagaimana drone dapat digunakan untuk penguntitan, pemantauan atau dokumentasi yang tidak sah. Pembuatan konten tanpa izin dapat dikategorikan sebagai kejahatan siber jika konten foto ataupun video yang termuat tersebut tidak memiliki izin dan disalahgunakan. Penelitian ini bertujuan untuk mengetahui bentuk pelanggaran privasi terkait penggunaan drone dan perlindungan hukum terhadap privasi korban penyalahgunaan pembuatan konten mengunakan drone. Metode penelitian dilakukan dengan metode penelitian hukum yuridis-normatif. Data yang digunakan dalam penelitian ini adalah data sekunder yang bersumber dari bahan hukum primer dan sekunder serta wawancara sebagai data pendukung. Kesimpulan yang didapat dari penelitian adalah pembuatan konten menggunakan drone menimbulkan beragam bentuk pelanggaran privasi serta aturan hukum yang belum mengatur secara spesifik terkait penggunaan drone. Adapun perlindungan hukum untuk korban pelanggaran hak privasi terhadap pembuatan konten menggunakan drone tertera dalam Undang-undang No. 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik yang mengatur tentang korban yang haknya dilanggar dapat menggugat dan menerima ganti rugi atas kerugian yang ditimbulkan serta mewajibkan pelaku untuk menghapus Informasi Elektronik dan /atau Dokumen Elektronik sesuai dengan ketentuan peraturan perundang-undangan.
Kata kunci: Drone, Konten tanpa izin, Korban, Pelanggaran privasi, Perlindungan hukum

Abstract

If drones are new, people have always been concerned about how they can be used for unauthorized stalking, monitoring, or documentation. Unauthorized content creation can be categorized as a cybercrime if the photo or video content contained does not have permission and is misused. This study aims to determine the form of privacy violations related to the use of drones and legal protection for the privacy of victims of misuse of content creation using drones. The research method was carried out using the juridical-normative legal research method. The data used in this study are secondary data sourced from primary and secondary legal materials and interviews as supporting data. The conclusion obtained from the study is that content creation using drones causes various forms of privacy violations and legal regulations that do not specifically regulate the use of drones. The legal protection for victims of violations of privacy rights against content creation using drones is stated in Law No. 1 of 2024 concerning Information and Electronic Transactions which regulates that victims whose rights are violated can sue and receive compensation for the losses incurred and require the perpetrator to delete Electronic Information and/or Electronic Documents in accordance with the provisions of laws and regulations.
Keywords: Drones, Unauthorized content, Victims, Privacy violations, Legal protection

I. Pendahuluan

Drone atau *unmanned aerial vehicle* adalah pesawat udara tanpa awak yang dikendalikan jarak jauh melalui remote oleh pilot baik secara manual atau otomatis. Sistem kerja *drone* agar bisa dikendalikan dalam jarak jauh adalah dengan menggunakan pancaran gelombang radio yang terhubung antara remote dan reseptor sinyal pada *drone* serta pemanfaatan hukum aerodinamika untuk membuat *drone* dapat terbang.[1] Selama *drone* menjadi sesuatu yang baru, masyarakat selalu khawatir tentang bagaimana *drone*

[1] Saroinsong, H. S., Poekoel, V. C., & Manembu, P. D. (2018). Rancang Bangun Wahana Pesawat Tanpa Awak (Fixed Wing) Berbasis Ardupilot. *Jurnal Teknik Elektro Dan Komputer, 7*(1), 73–84. Hlm.4

dapat digunakan untuk penguntitan, pemantauan, atau dokumentasi yang tidak sah. *Drone* dengan ukurannya yang cukup kecil bisa terbang di mana saja tanpa mudah terdeteksi.

Perkembangan pembuatan konten menggunakan *drone* melahirkan berbagai tindakan kriminal yang dapat merugikan korban secara materiil maupun immateriil. Kasus penyalahgunaan konten menggunakan kamera dan *drone* marak terjadi di masyarakat. Contohnya, kasus perekaman sembunyi-sembunyi terhadap ibu hamil di KRL pada Oktober 2023 yang berujung viral dan tragis.[2] Kasus lain terjadi di Utah pada 2017, di mana *drone* digunakan untuk merekam aktivitas pribadi seseorang tanpa izin di kediamannya.[3] Pengambilan konten tanpa izin dapat dikategorikan sebagai kejahatan siber jika foto atau video yang diambil tersebut diunggah ke media sosial untuk keuntungan pribadi tanpa izin dan merugikan orang lain. Kejahatan siber adalah perbuatan melawan hukum yang dilakukan dengan memanfaatkan teknologi komputer dan telekomunikasi sebagai alat demi keuntungan pribadi dengan merugikan orang lain.[4] Kejahatan siber memiliki cakupan sangat luas dengan beragam cara yang dapat dilakukan oleh pelaku untuk mengincar korbannya.[5]

Melihat risiko dan maraknya penyalahgunaan pengambilan konten terutama dalam penggunaan *drone* maka pengambilan konten melalui *drone* perlu diatur secara ketat. Pengambilan konten melalui *drone* tidak dapat dilakukan dengan sembarangan dan harus sesuai dalam Peraturan Menteri Perhubungan (Permenhub) Nomor 37 Tahun 2020 tentang Pengoperasian Pesawat Udara Tanpa Awak Di Ruang Udara Yang Dilayani Indonesia. Berdasarkan Permenhub tersebut diketahui bahwa *drone* hanya boleh dioperasikan sesuai dengan ketentuan perundang-undangan. Pengambilan konten melalui *drone* harus memiliki izin dengan pihak terlibat agar tidak melanggar hak asasi manusia seperti hak privasi dan hak perlindungan data pribadi.

Hak pribadi adalah bentuk hak yang mendasar bagi setiap individu untuk hidup tanpa intervensi dari pihak manapun. Hak tersebut mencakup kebebasan dari gangguan, pengawasan, atau campur tangan yang tidak diinginkan dalam kehidupan pribadi seseorang.[6] Dalam konteks ini, setiap orang berhak atas ruang pribadi yang bebas dari pengintaian, pemantauan, atau tindakan apapun yang dapat mengganggu ketenangan dan kenyamanan hidup mereka.[7] Hak pribadi meliputi berbagai aspek kehidupan termasuk hak atas privasi, hak untuk membuat keputusan pribadi tanpa paksaan, dan hak untuk melindungi informasi pribadi dari penyalahgunaan.[8] Perlindungan terhadap hak pribadi sangat penting dalam menjaga martabat dan integritas individu, serta menciptakan lingkungan yang aman dan harmonis di mana setiap orang dapat menikmati kebebasan mereka secara penuh.[9] Tanpa perlindungan yang memadai terhadap hak pribadi, individu dapat menjadi rentan terhadap berbagai bentuk pelanggaran dan eksploitasi yang dapat merugikan mereka secara fisik, emosional, dan psikologis. Perlindungan hukum atas hak pribadi sangat diperlukan bagi siapa pun dan negara sebagai pelaksana kebijakan sudah seharusnya bertangung jawab atas perlindungan hak-hak dasar perlindungan privasi tersebut sebagaimana telah diamanatkan dalam Pasal 28 G ayat (1) Undang-Undang Dasar 1945.

Hak pribadi termasuk dalam bagian perlindungan hak asasi terhadap hak-hak privasi atau hak-hak privat untuk mencegah terjadinya perlakuan diskriminasi.[10] Hak privasi pada setiap orang sebagaimana termuat dalam Pasal 28G ayat (1) Undang-Undang Dasar (UUD) Negara Republik Indonesia Tahun 1945 menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman

---

[2] Dian, R. (2023). Ibu Hamil Yang Direkam Tanpa Izin Alami Keguguran Saat Turun Dari KRL. Diakses pada 30 Desember 2023, https://narasi.tv/read/narasi-daily/viral-ibu-hamil-direkam-tanpa-izin-di-krl.

[3] Crawford, J. (2018). 10 Crimes Committed Using A Drone. Diakses pada 30 Desember 2023, https://listverse.com/2018/07/26/10-crimes-committed-using-a-drone/.

[4] Marufah, N., Rahmat, H.K., & Widana, D. K. K. I. (2020). Degradasi Moral Sebagai Dampak Kejahatan Siber Pada Generasi Millenial Di Indonesia. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial, 7*(1), 191–201. Hlm.4

[5] Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Technology and Economics Law Journal, 2*(2). Hlm.3.

[6] Ningsih, C. S., et al. (2021). Hak Kebebasan Berpendapat Yang Semakin Menyempit Dan Memburuk. *Jurnal Syntax Fusion, 1*(2), 25–39. Hlm,4

[7] Prastyanti, R. A. (2020). Perlindungan Keamanan Siber Berdasarkan Perspektif Hak Asasi Manusia. *Prosiding Seminar Nasional Hukum, Bisnis, Sains Dan Teknologi*, *1*, 275. Hlm.3.

[8] Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik. *Jurnal Ham, 11*(2), 285–99. Hlm 107

[9] Husna, S. K. I., & Najicha, F. U. (2023). Pancasila Dan Hubungannya Dengan Hak Asasi Manusia Di Indonesia. *Civic Education: Media Kajian Pancasila Dan Kewarganegaraan, 7*(2), 104–12. Hlm.3.

[10] Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *Jatiswara, 34*(3), 239–249. Hlm 3.

ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi manusia. Perlindungan hak privasi juga diatur melalui Pasal 26 ayat 1 Undang-undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik yang menyatakan bahwa setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan kecuali ditentukan lain oleh peraturan perundang-undangan.

Kaitannya perlindungan privasi dengan *drone* adalah tidak adanya aturan yang mengatur secara khusus mengenai hukuman penyalahgunaan penggunaan *drone* yang digunakan untuk membuat konten tanpa izin dan persetujuan dari pihak-pihak tidak berkepentingan yang ikut terekam. Dampak negatif dari penggunaan *drone* tanpa izin dapat mengancam privasi individu dan dapat dipergunakan untuk memata-matai serta mengancam keamanan dan keselamatan negara. Tingginya kasus kejahatan siber terkait pembuatan konten dan ancaman penyalahgunaan konten menggunakan *drone* menimbulkan urgensi untuk memahami penyebab dan dampak dari permasalahan sehingga perlindungan hukum bagi korban penyalahgunaan konten yang diambil melalui *drone* menjadi aspek yang penting untuk diteliti.

II. Metode Penelitian

Penelitian dilakukan melalui jenis penelitian yuridis-normatif dengan melakukan pencarian bahan hukum, mengidentifikasi asas-asas hukum untuk mencari sumber data yang dibutuhkan. Data sekunder yang dikumpulkan meliputi bahan hukum atau data tertulis yang tidak terbatas pada peraturan perundang-undangan, buku, majalah, artikel dan sumber tertulis lainnya sesuai dengan fokus penelitian yang dikaji. Pendekatan kualitatif preskriptif dalam penelitian digunakan dengan melibatkan proses penyaringan, pengolahan, dan penarikan kesimpulan dari aspek-aspek penting yang terdapat dalam data yang berhasil dikumpulkan. Hasil analisis tersebut kemudian dideskripsikan secara singkat dan terstruktur sehingga diperoleh kesimpulan yang dapat memberikan jawaban terhadap permasalahan yang menjadi fokus dalam penelitian ini.

III. Hasil dan Pembahasan

3.1. Bentuk Pelanggaran Privasi terkait Penggunaan *Drone*

Penggunaan *drone* dalam berbagai bidang telah membuka potensi baru dalam pelanggaran privasi. *Drone* memiliki perbedaan dari kebanyakan sistem pengawasan lainnya berdasarkan sejumlah aspek. Pertama *drone* memberikan sudut pandang udara yang menunjang kemampuannya untuk melewati medan yang sulit. Kedua *drone* juga dapat memperbesar suatu gambar yang terpantau melalui kamera. Ketiga *drone* dapat mengangkut beban muatan tertentu. Keempat *drone* tidak terlalu mencolok seperti CCTV untuk melakukan pengintaian atau pengawasan. Kelima *drone* mampu terbang dengan kebisingan yang lebih rendah daripada helikopter.[11] Aspek-aspek tersebut membuat kekhawatiran akan potensi pelanggaran privasi yang terjadi dengan menggunakan *drone* semakin meningkat sebagaimana disadari oleh Anggota Parlemen Eropa yang mengatakan *"when combined with technologies and applications, change and transform the nature of surveillance, magnifying it, when compared to other similar tools (satellites, aircrafts, helicopters, CCTV)."*[12]

Menurut data yang dihimpun oleh Asosiasi Sistem & Teknologi Tanpa Awak (ASTTA) pada tahun 2021, terdapat sekitar 90 ribu *drone* komersial dengan harga di bawah Rp20 juta yang beredar di pasaran. *Drone* komersial adalah *drone* yang digunakan untuk keperluan pribadi bukan sebagai sumber pencaharian. *Drone* industri yang beredar dengan harga di atas Rp20 juta berkisar antara 5.000 hingga 10.000-unit yang sebagian besar didominasi oleh produk asing. *Drone* industri adalah *drone* yang digunakan untuk mendukung kegiatan kerja baik oleh perusahaan ataupun perorangan.[13]

Data peredaran *drone* di pasaran menunjukkan atensi yang tinggi atas penggunaan *drone* di Indonesia. Peningkatan kuantitas dalam penggunaan *drone* harus diiringi dengan kesadaran penuh akan berbagai

[11] Algar, J. (2014). DARPA Wants Drones to Be Swift as Hawks, Small as Insects. Diakses pada 30 Desember 2023, https://www.techtimes.com/articles/23876/20141230/darpa-wants-drones-to-be-swift-as-hawks-small-as-insects.htm.
[12] Bassi, E. (2019). European Drones Regulation: Today's Legal Challenges. *2019 International Conference on Unmanned Aircraft Systems (ICUAS),* IEEE, 443–50. Hlm.6
[13] Ibid. Rusti Dian

potensi penyalahgunaan yang mungkin timbul kedepan termasuk pelanggaran hak privasi. Pelanggaran hak privasi penggunaan *drone* didasari oleh beberapa alasan, antara lain:[14]

a. Pelaku yakin telah melakukan hal yang benar, bahwa mereka berhak mengawasi seseorang atau bahwa seseorang adalah milik mereka dengan cara tertentu.

b. Pelaku tidak tahu atau tidak peduli apa dampak perilakunya terhadap seseorang.

c. Pelaku mampu merasionalisasi tindakannya sampai tingkat tertentu dan tidak berpikir bahwa tindakan mereka merupakan sesuatu yang salah atau tidak biasa.

Bentuk ancaman pelanggaran privasi menggunakan *drone* telah menjadi isu yang semakin memprihatinkan dalam masyarakat *modern*, seiring dengan kemajuan teknologi dan penetrasi yang semakin luas dari *drone* dalam berbagai aspek kehidupan manusia. *Drone* dengan kemampuannya yang semakin canggih dan terjangkau telah menjadi alat yang potensial untuk melanggar privasi individu secara signifikan dan memperluas cakupan potensi bahaya yang dapat ditimbulkannya. Harga yang semakin terjangkau dan ketersediaan yang semakin meluas menjadikan *drone* tidak lagi eksklusif bagi pemerintah atau organisasi besar karena dapat dimiliki dan dioperasikan oleh individu atau kelompok kecil sehingga meningkatkan risiko pelanggaran privasi yang tidak terkendali. Berikut ini adalah beberapa bentuk ancaman pelanggaran privasi menggunakan *drone* yang dibedakan dalam tujuh bentuk antara lain:

a. Privasi seseorang

   Algoritme pengenalan wajah dapat berjalan di server yang dikirimkan oleh tautan video dari *drone* untuk membantu mengidentifikasi individu.

b. Privasi keseharian seseorang

   Drone dapat memantau apa yang dilakukan seseorang dengan menggunakan kamera optik atau termal atau pencitraan inframerah.

c. Privasi dari data visual yang diambil

   Drone dapat mengumpulkan dan mengirimkan gambar-gambar pribadi seseorang.

d. Privasi komunikasi

   Drone dapat membawa mikrofon untuk merekam apa yang dikatakan seseorang.

e. Privasi dari lokasi atau tempat tinggal

   Drone dapat mengikuti ke mana seseorang pergi dan menggunakan muatan *global positioning system* (GPS) untuk mengirimkan lokasi orang tersebut.

f. Privasi dari pikiran dan perasaan seseorang

   Drone tidak dapat menembus pikiran tetapi operator *drone* dapat membuat beberapa asumsi tentang bagaimana perasaan seseorang dari ekspresi kemarahan atau kebahagiaan atau perasaan lainnya yang terekam oleh *drone*.

g. Privasi kelompok

   Drone dapat memantau kelompok misalnya dalam demonstrasi, pawai, atau pertemuan.

Beberapa ancaman tersebut menjadikan *drone* memiliki risiko besar terhadap terjadinya pelanggaran privasi yang serius apabila digunakan dengan tidak sesuai. Bentuk ancaman privasi yang beragam dalam penyalahgunaan pembuatan konten menggunakan *drone* menciptakan kesulitan baru dalam melindungi keamanan dan privasi data pribadi di era teknologi yang berkembang pesat. Penggunaannya yang meluas dan kemampuan pemantauan yang canggih meningkatkan beragam macam risiko mulai dari kemungkinan kejahatan dan pelanggaran keamanan yang diakibatkan oleh penggunaan *drone* yang tidak etis, pengawasan yang tidak sah, pencurian data pribadi, penyusupan, dan pengintaian. Berdasarkan hal tersebut maka pelanggaran privasi yang dapat terjadi terkait penggunaan *drone*, antara lain:

[14] Bev, G. (2023). I'm Being Watched: How to Deal With Stalkers and Spies. Diakses pada 15 Desember 2023, https://owlcation.com/social-sciences/Somebody-is-Watching-Me.

a. Pengawasan yang Tidak Sah:[15]

Drone memiliki kemampuan yang sangat baik dalam megambil citra visual di udara dan melakukan pengawasan di udara.[16] Kemampuan *drone* untuk dapat melakukan pengawasan di udara juga dapat disalahgunakan untuk melakukan pengawasan yang tidak sah atau tidak diinginkan. Pengawasan tersebut mencakup pemantauan individu atau kelompok tanpa izin baik untuk tujuan komersial, keamanan, atau lainnya. Pelanggaran yang terjadi mencakup pengawasan rumah tangga, tempat kerja, atau bahkan ruang publik tanpa izin yang sesuai.[17] Pasal 27A Undang-undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik mengatur tentang perlindungan kehormatan yang menyatakan bahwa setiap orang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya hal tersebut diketahui umum dalam bentuk Informasi Elektronik dan/ atau Dokumen Elektronik yang dilakukan melalui Sistem Elektronik.

Pasal 45 ayat 4 Undang-undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik mengatur tentang sanksi pidana dan denda yang dapat dijatuhkan terhadap pelanggaran pasal 27A Undang-undang Nomor 1 Tahun 2024. Pasal 45 ayat 4 menyebutkan bahwa setiap orang yang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya hal tersebut diketahui umum dalam bentuk Informasi Elektronik dan/ atau Dokumen Elektronik yang dilakukan melalui Sistem Elektronik sebagaimana dimaksud dalam Pasal 27A dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/ atau denda paling banyak Rp400.000.000,00 (empat ratus juta rupiah).

b. Pengintaian dan penyusupan:

Drone dapat digunakan untuk pengintaian atau penyusupan ke dalam lingkungan pribadi, seperti halaman belakang rumah seseorang sehingga penggunaan *drone* dapat meningkatkan risiko pengintaian atau penyusupan yang tidak terdeteksi. Tindakan mengintai, mengikuti, atau merekam aktivitas seseorang secara diam-diam sebelumnya belum diatur secara khusus dalam KUHP lama dan baru diatur dalam KUHP baru. Tindakan pengintaian dan penyadapan telah diatur secara khusus dalam Pasal 259 KUHP baru yang mengatur bahwa pengintaian dan penyadapan termasuk tindakan yang dapat dikenai sanksi hukum sebagaimana berikut:

Dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak kategori VI, Setiap orang yang:

1) Mempergunakan kesempatan yang diperoleh dengan tipu muslihat atau secara melawan hukum merekam gambar seseorang atau lebih yang berada di dalam suatu rumah atau ruangan yang tidak terbuka untuk umum dengan menggunakan alat bantu teknis sehingga merugikan kepentingan hukum orang tersebut;
2) Memiliki gambar yang diketahui atau patut diduga diperoleh melalui perbuatan sebagaimana dimaksud dalam huruf a; atau
3) Menyiarkan atau menyebarluaskan gambar sebagaimana dimaksud dalam huruf b dengan menggunakan sarana teknologi informasi

Unsur perbuatan yang dilanggar oleh pilot *drone* atau seseorang yang menggunakan *drone* untuk merekam secara diam-diam dalam pasal 259 KUHP antara lain:

1) Mempergunakan kesempatan yang diperoleh dengan tipu muslihat atau secara melawan hukum. Pengoperasian *drone* digunakan untuk merekam secara diam-diam termasuk kedalam unsur mempergunakan kesempatan secara melawan hukum sesuai dengan peraturan perundang-undangan.
2) Merekam gambar seseorang atau lebih yang berada di dalam suatu rumah atau ruangan yang tidak terbuka untuk umum. Pengoperasian *drone* pada umumnya digunakan untuk memperoleh gambar visual di udara, selain itu keunggulannya yang dapat terbang hingga ketinggian tertentu dapat dimanfaatkan untuk mengambil gambar atau video seseorang yang berada di ruang tidak terbuka.

[15] Khan, M. A., et al. (2022). On the Detection of Unauthorized Drones—Techniques and Future Perspectives: A Review. *IEEE Sensors Journal, 22*(2), 11439–55. Hlm.2.
[16] Boštjan, S. (2016). Drones in (Slovene) Criminal Investigation. *Kriminalistička Teorija i Praksa*, *3(*2), 7–25. Hlm.10.
[17] Choi, Y. J. (2022). Security Threat Scenarios of Drones and Anti-Drone Technology. *Academy of Strategic Management Journal, 21*(1), 1–7. Hlm.2.

3) Menggunakan alat bantu teknis sehingga merugikan kepentingan hukum orang tersebut. Pengoperasian *drone* termasuk kedalam alat bantu teknis yang dapat digunakan seseorang sehingga merugikan kepentingan hukum atau melanggar hak privasi orang lain.

Penggunaan Pasal KUHP baru dalam bagian ini untuk memberikan edukasi sekaligus sosialisasi dari masa transisi peralihan KUHP lama menjadi KUHP baru yang diberlakukan selama 3 tahun agar masyarakat dan penegak hukum dapat beradaptasi dengan KUHP baru dan memahami bahwa telah ada peraturan yang mengatur secara khusus mengenai tindakan penguntitan.

c. Penggunaan untuk kejahatan:[18]

Drone juga dapat digunakan sebagai alat untuk melakukan kejahatan, seperti pemantauan yang intensif untuk merencanakan kejahatan, menyebarkan bahan ilegal untuk merusak suatu ekosistem lingkungan, membawa muatan berbahaya seperti bahan peledak atau bahkan melakukan pembunuhan.[19] Posisi *drone* sebagai teknologi baru haruslah disamakan dengan alat-alat pendukung tindak pidana dalam perspektif hukum pidana, seperti pisau, benda tumpul atau hal lain agar pelaku yang telah memenuhi unsur tindak pidana dalam suatu pasal dapat dijatuhi pidana setimpal dengan perbuatannya (*Culpae poena par esto*).

d. Pelanggaran keamanan:

Penggunaan *drone* secara tidak sah atau tidak etis juga dapat mengancam keamanan individu atau kelompok sehingga meningkatkan risiko pencurian informasi rahasia. Penggunaan *drone* juga dapat mengidentifikasi kerentanan keamanan, atau melakukan serangan fisik atau *cyber*. Pasal 28G ayat (1) UUD 1945 menyatakan bahwa Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.

e. Pelanggaran privasi yang berkelanjutan:

Drone yang dipasang dengan teknologi canggih seperti kamera optik atau termal, sensor gerak, atau sistem pengenalan wajah dapat menciptakan pelanggaran privasi yang berkelanjutan. *Drone* dapat terus memantau atau mengidentifikasi individu atau kelompok tanpa henti. Pola perilaku yang terus berulang untuk memantau pergerakan atau mengidentifikasi suatu individu atau kelompok dapat termasuk kedalam sebuah tindak pidana.

f. Kesalahan dan tanggung jawab:

Kitab Undang-Undang Hukum Pidana (KUHP) menguraikan unsur-unsur tindak pidana kedalam dua jenis, yaitu unsur objektif dan unsur subjektif. Unsur objektif berkaitan dengan keadaan dimana pelaku harus melakukan tindakannya, sedangkan unsur subjektif yaitu menyangkut sisi batin pelaku, sengaja (*dolus*) dan tidak sengaja (*culpa*).[20] Perilaku pelaku untuk melakukan pendekatan secara visual, mengikuti berkali-kali dapat membuat seseorang merasa terganggu, takut, dan terancam keselamatannya.

g. Ketidakamanan *drone* itu sendiri:

Pelanggaran privasi dapat terjadi jika *drone* diretas atau diambil alih oleh pihak yang tidak sah, yang dapat digunakan untuk tujuan yang tidak senonoh atau bahkan berbahaya. Peretasan *drone* meliputi proses manipulasi data GPS, gangguan atau manipulasi transmisi *drone*, memanipulasi rekaman yang ditangkap, menyuntikkan atau menginput data sensor yang dipalsukan, menginfiltrasi *drone* dengan perangkat keras atau dan perangkat lunak berbahaya, menyerang sistem penugasan misi *drone*, pengungkapan komunikasi yang tidak sah, dan gangguan atau manipulasi sinyal kontrol *remote drone*.[21]

3.2. Perlindungan Hukum terhadap Privasi Seseorang yang Menjadi Korban Penyalahgunaan *Drone* dalam Pembuatan Konten

[18] Ramadhan, M. A., & Fikri, R. (2024). Penggunaan Drone dalam Kejahatan: Tinjauan Terhadap Penggunaan Teknologi UAV untuk Pencurian Data dan Serangan Fisik. *Jurnal Media Akademik (JMA), 2*(6). Hlm.2

[19] Sarjito, A., & Lelyana, N. (2023). Analisis Dampak Persepsi Ancaman Drone Terhadap Pembuatan Kebijakan Pertahanan Dan Proses Alokasi Sumber Daya. *Jurnal of Management and Social Sciences, 1*(4), 14–32. Hlm.25.

[20] Sinaga, A. Br., Usman, U., & Wahyudhi, D. (2021). Perbuatan Menguntit (Stalking) Dalam Perspektif Kebijakan Hukum Pidana Indonesia. *PAMPAS: Journal of Criminal Law, 2*(2), 15–28. Hlm.19

[21] Rugo, A., Ardagna, C. A., & Ioini, N. E. (2022). A Security Review in the UAVNet Era: Threats, Countermeasures, and Gap Analysis. *ACM Computing Surveys (CSUR), 55*(1), 1–35. Hlm.10.

Penggunaan *drone* telah meluas dari sektor militer menuju sektor komersial, dan rekreasi sejak diperkenalkannya *Drone Parrot AR* pada tahun 2008.[22] Berdasarkan data yang dihimpun oleh Asosiasi Sistem & Teknologi Tanpa Awak (ASTTA), jumlah pilot komersial per 1 Agustus 2021 sebanyak 50.000 orang pilot. Dari jumlah tersebut hanya sekitar 2.500 atau 5% yang sudah memiliki lisensi dari Kementerian Perhubungan, selebihnya baru akan mengikuti atau masih dalam proses pembuatan lisensi.[23]

Kewajiban pendaftaran *drone* serta lisensi pilot *drone* diperlukan dalam penerbangan *drone.* Kewajiban tersebut menjadi standar yang memberikan jaminan bahwa seseorang telah mengetahui standar operasional serta kewajibannya ketika mengoperasikan *drone* sehingga dapat mengurangi tingkat kecelakaan dan pelanggaran privasi. Pernyataan tersebut berbanding terbalik dengan beberapa fenomena yang terjadi terkait penyalahgunaan penggunaan *drone* mulai dari *drone* yang jatuh ditempat umum, *drone* yang masuk kedalam wilayah Kawasan Keselamatan Operasi Penerbangan (KKOP) hingga *drone* yang dipaksa turun karena berpotensi mengganggu keamanan dan melanggar privasi sebagaimana yang dapat digambarkan dalam tabel pelanggaran dan penyalahgunaan *drone* berikut ini:

Tabel 1. Kasus Pelanggaran dan Penyalahgunaan *Drone* di Indonesia dan Luar Negeri

Nomor	Tahun	Pelanggaran dan Penyalahgunaan *Drone*	Tempat
1	2015	Sebuah *drone* jatuh di Menara BCA Bundaran Hotel Indonesia yang merupakan kawasan padat aktivitas	Hotel Indonesia
2	2018	4 Kasus *drone* melanggar Kawasan Keselamatan Operasi Penerbangan (KKOP) dengan masuk ke area bandara yaitu Bandara Balikpapan, Bandara Depati Amir Pangkal Pinang, dan dua kejadian di Bandara Halim	Bandara Balikapan, Bandara Depati Amir Pangkal Pinang, Bandara Halim
3	2018	Helikopter mendarat darurat akibat menghindari *drone* di South Carolina, Amerika Serikat	Amerika Serikat
4	2018	*Drone* digunakan teroris untuk melakukan percobaan pembunuhan Presiden Venezuela	Venezuela
5	2024	Polda Sumatera Utara memaksa turun delapan *drone* yang terbang tanpa izin di *venue* F1 *Powerboat*, Balige, Sumatera Utara	Sumatera Utara

Sumber: Data ini didapat dari berbagai sumber

Penyalahgunaan dan pelanggaran tersebut terjadi karena kelalaian individu dalam mematuhi aturan, batasan, serta pengetahuan dasar yang dibutuhkan dalam menerbangkan *drone*. Bentuk perlindungan hukum terhadap korban penyalahgunaan atau pelanggaran privasi menggunakan *drone* dapat di analisa menggunakan pendekatan perlindungan hukum represif dan pendekatan perlindungan hukum preventif. Perlindungan hukum represif lebih menekankan pada undang-undang yang dapat digunakan untuk menjatuhkan sanksi pidana kepada pelaku pelanggaran menggunakan *drone*, sedangkan perlindungan hukum preventif lebih menekankan kepada undang-undang yang digunakan untuk memberikan rambu-rambu atau batasan-batasan dalam melakukan suatu perbuatan yang melanggar atau dengan pendekatan-pendekatan lain dalam upaya mengedukasi masyarakat untuk memahami batasan-batasan yang telah diatur dalam perundang-undangan dan mencegah terjadinya kejahatan.

a. Perlindungan Hukum Represif

Drone sebagai alat yang memiliki kemampuan untuk melakukan pengambilan konten di udara berpotensi menimbulkan berbagai ancaman terutama melanggar privasi individu yang ada di bawahnya. Privasi adalah hak untuk bisa merasa nyaman, aman, tidak terganggu. Penggunaan *drone* harus melihat batas-batas privasi, apakah penggunaan *drone* melampaui batas-batas privasi seseorang, kemudian apabila penggunaan *drone* bersifat *urgent* maka harus disertai dengan izin atau dilakukan oleh seseorang yang memiliki kewenangan tertentu, memiliki dasar hukum yang sah untuk melakukan penegakan hukum atau investigasi yang diberikan oleh undang-undang secara sah. Belum adanya pasal yang mengatur tentang bentuk perlindungan hukum terhadap korban penyalahgunaan atau pelanggaran privasi

[22] Birnbach, S., Baker, R., & Martinovic, I. (2017). Wi-Fly?: Detecting Privacy Invasion Attacks by Consumer Drones. *NDSS.* Hlm.13.

[23] Hakim, D. (2022). Outlook Industri Drone Indonesia 2023. Diakses pada 20 Mei 2024, https://astta.id/2022/11/24/outlook-industri-drone-indonesia-2023/.

menggunakan *drone* dalam Kitab Undang-Undang Hukum Pidana menjadi tantangan bagi aparat penegak hukum untuk memberikan perlindungan hukum, menerapkan kebijakan dan menjatuhkan sanksi terhadap penyalahgunaan atau pelanggaran privasi menggunakan *drone*. Pendekatan melalui peraturan perundang-undangan dan konvensi internasional yang mengatur penyalahgunaan atau pelanggaran privasi serupa yang dapat dilakukan oleh *drone* bisa digunakan untuk memberikan perlindungan dan kepastian hukum.

Drone yang digunakan untuk mengamati dan merekam secara *ilegal* dapat dikenakan perbuatan *illegal interception*. Perbuatan *illegal interception* termasuk dalam bentuk *cybercrime* pada *Convention on Cyber Crime* tanggal 23 November 2001 di kota Budapest Hongaria.[24] Kualifikasi *cybercrime* menurut *Convention on Cyber Crime* 2001 di Budapest Hongaria antara lain:[25]

1) *Ilegal acces* (Akses terlarang) mengacu pada pelanggaran atau penyusupan yang disengaja ke dalam sistem komputer tanpa otorisasi.
2) *Ilegal interception* (Penyadapan ilegal) mengacu pada pengambilan data komputer yang disengaja dan tidak sah yang tidak dimaksudkan untuk akses publik ke, dari, atau di dalam sistem komputer dianggap sebagai penyadapan ilegal. Hal tersebut terjadi ketika alat bantu teknis digunakan untuk memfasilitasi penyadapan.
3) *Data interference* (Gangguan data) mengacu pada penghancuran, modifikasi, pemindahan, atau penghapusan data komputer yang disengaja dan tidak sah.
4) *System interference* (Gangguan sistem) yang mengacu pada halangan atau gangguan yang disengaja dan tidak sah terhadap pengoperasian sistem komputer tanpa otorisasi yang diperlukan.
5) *Device Misuse* (Penyalahgunaan Perangkat) khususnya penggunaan perangkat keras komputer secara tidak sah, yang mencakup kode akses, program komputer, dan kata sandi.
6) *Computer-related forgery* (Pemalsuan yang berhubungan dengan komputer) khususnya pemalsuan (penyisipan, modifikasi, atau penghapusan data yang sah dengan maksud untuk menggunakannya sebagai data yang autentik padahal tidak memiliki otorisasi yang diperlukan).
7) *Computer-Related Fraud*, yaitu kegiatan penipuan yang menyebabkan hilangnya barang atau kekayaan orang lain dengan cara memasuki, mengubah, menghapus data komputer, atau mengganggu pengoperasian komputer atau sistem komputer, tanpa otorisasi dan dengan maksud untuk mendapatkan keuntungan ekonomi bagi diri sendiri atau orang lain.

Illegal interception tertera pada Pasal 31 ayat (1) dan (2) Undang-undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik yang menyatakan bahwa:

1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain.
2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

Penjelasan "intersepsi atau penyadapan" adalah kegiatan untuk mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, seperti pancaran elektromagnetis atau radio frekuensi. Perbuatan *ilegal interception* dapat dilakukan oleh *drone* dengan cara menampilkan rekaman secara *real time* atau *live stream*. Penggunaan tersebut marak dilakukan dalam perang untuk menampilkan keadaan medan perang secara *real time*, menemukan posisi musuh dan memantau pergerakan musuh tanpa mempertaruhkan nyawa pasukan.[26]

[24] Alfian, M. (2018). Penguatan Hukum Cyber Crime Di Indonesia Dalam Perspektif Peraturan Perundang-Undangan. *Kosmik Hukum, 17*(2). Hlm.3.
[25] Ibid. Alfian
[26] Kunertova, D. (2023). The War in Ukraine Shows the Game-Changing Effect of Drones Depends on the Game. *Bulletin of the Atomic Scientists, 79*(2), 95–102. Hlm.97.

Selaras dengan Pasal 31 Undang-undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik perbuatan penyadapan diatur dalam Pasal 258 Kitab Undang-Undang Hukum Pidana baru yang menyatakan bahwa:

1) Setiap orang yang secara melawan hukum mendengarkan, merekam, membelokkan, mengubah, menghambat, dan/ atau mencatat transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, dipidana dengan pidana penjara paling lama l0 (sepuluh) tahun atau pidana denda paling banyak kategori VI.
2) Setiap orang yang menyiarkan atau menyebarluaskan hasil pembicaraan atau perekaman sebagaimana dimaksud pada ayat (1), dipidana dengan pidana penjara paling lama l0 (sepuluh) tahun atau pidana denda paling banyak kategori VI.
3) Ketentuan sebagaimana dimaksud pada ayat (1) tidak berlaku bagi setiap orang yang melaksanakan ketentuan peraturan perundang-undangan atau melaksanakan perintah jabatan sebagaimana dimaksud dalam Pasal 31 dan Pasal 32.

Penyalahgunaan penggunaan *drone* untuk melakukan penguntitan dapat dikenai ketentuan Pasal 259 KUHP yang menyatakan bahwa:

Dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak kategori VI, Setiap orang yang:

1) Mempergunakan kesempatan yang diperoleh dengan tipu muslihat atau secara melawan hukum merekam gambar seseorang atau lebih yang berada di dalam suatu rumah atau ruangan yang tidak terbuka untuk umum dengan menggunakan alat bantu teknis sehingga merugikan kepentingan hukum orang tersebut;
2) Memiliki gambar yang diketahui atau patut diduga diperoleh melalui perbuatan sebagaimana dimaksud dalam huruf a; atau
3) Menyiarkan atau menyebarluaskan gambar sebagaimana dimaksud dalam huruf b dengan menggunakan sarana teknologi informasi.

Pasal dalam KUHP baru pada bagian ini dimaksudkan untuk memberikan edukasi selama masa transisi. Tujuannya adalah agar masyarakat dan penegak hukum dapat beradaptasi dengan peraturan baru tersebut. Pasal ini secara khusus mengatur tentang tindakan penguntitan dan penyadapan guna memastikan bahwa semua pihak memahami dan mematuhi ketentuan yang telah diatur dalam KUHP yang baru.

b. Perlindungan hukum preventif

Perlindungan hukum preventif merupakan upaya yang dilakukan untuk mencegah terjadinya pelanggaran hukum sebelum masalah tersebut terjadi. Upaya ini dilakukan melalui regulasi yang ketat, kampanye kesadaran dalam penggunaan teknologi. Perlindungan hukum preventif bertujuan untuk menciptakan lingkungan yang aman dan teratur, sehingga masyarakat dapat menjalani aktivitasnya dengan lebih nyaman dan terlindungi dari berbagai potensi kejahatan atau pelanggaran hukum. Tujuan perlindungan hukum tersebut dapat tercapai melalui tiga pendekatan utama yaitu pendekatan hukum, pendekatan sosial, dan pendekatan teknologi.

1) Pendekatan hukum

Pendekatan hukum adalah dasar dari perlindungan hukum preventif. Pendekatan tersebut melibatkan pembuatan dan penegakan peraturan perundang-undangan yang mengatur penggunaan dan pemanfaatan teknologi seperti *drone*. Melalui regulasi yang jelas dan tegas, pemerintah dapat menetapkan batasan-batasan yang harus dipatuhi oleh individu maupun organisasi. Misalnya pengaturan pengoperasian *drone,* peraturan yang mengatur ketinggian penerbangan, area terlarang, dan persyaratan izin dapat membantu mencegah penyalahgunaan yang dapat mengganggu privasi atau keselamatan publik. Perlindungan hukum hak privasi didasari oleh Pasal 28G ayat (1) UUD 1945 yang menyebutkan bahwa Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya, serta atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.

Perlindungan hukum hak privasi korban penyalahgunaan pembuatan konten menggunakan *drone* tertera dalam Pasal 29 Undang-undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia yang menyatakan bahwa:

(a) Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya.

(b) Setiap orang berhak atas pengakuan di depan hukum sebagai manusia pribadi di mana saja ia berada.

Pasal 30 Undang-undang Nomor 39 Tahun 1999 juga mengatur tentang perlindungan hukum hak privasi korban bahwa setiap orang berhak atas rasa aman dan tentram serta perlindungan terhadap ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu.

Perlindungan hukum seseorang yang merasa telah dirugikan akibat pembuatan konten, perekaman secara diam-diam menggunakan *drone* atau bentuk lain secara luas dapat menggunakan Pasal 26 Undang-undang Informasi dan Transaksi Elektronik mengenai perlindungan data pribadi bagian dari hak pribadi (*privacy rights*). Hak untuk dilupakan atau *the right to forgotten* tertera dalam pasal tersebut menyebutkan bahwa:

(a) Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan.

(b) Setiap orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini.

(c) Setiap penyelenggara sistem elektronik wajib menghapus informasi elektronik dan/atau dokumen elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan orang yang bersangkutan berdasarkan penetapan pengadilan.

(d) Setiap penyelenggara sistem elektronik wajib menyediakan mekanisme penghapusan informasi elektronik dan/ atau dokumen elektronik yang sudah tidak relevan sesuai dengan ketentuan peraturan perundang-undangan.

(e) Ketentuan mengenai tata cara penghapusan informasi elektronik dan/atau dokumen elektronik sebagaimana dimaksud pada ayat (3) dan ayat (4) diatur dalam peraturan pemerintah

Pasal 5 Undang-undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban menguraikan hak-hak yang dimiliki oleh korban dan saksi, termasuk perlindungan atas harta benda, keamanan pribadi, dan keluarganya. Korban berhak untuk terlibat dalam pemilihan dan penentuan jenis bantuan keamanan dan perlindungan serta memastikan jenis dukungan dan perlindungan keamanan yang dibutuhkan korban sebagai pihak yang paling dirugikan. Pasal 7A Undang-undang Nomor 31 Tahun 2014 menjelaskan bagaimana korban tindak pidana memiliki hak untuk memperoleh restitusi yang berupa ganti rugi secara materiil maupun immateriil.

Bentuk perlindungan hukum atas penggunaan *drone* yang lain diatur dalam Peraturan Menteri Perhubungan (Permenhub) Nomor 63 Tahun 2021 dan Peraturan Menteri Perhubungan (Permenhub) Nomor 37 Tahun 2020. Peraturan tersebut mencakup ketentuan tentang izin operasional, area terlarang untuk penerbangan *drone*, dan batasan-batasan lain yang bertujuan untuk memastikan bahwa penggunaan *drone* tidak mengganggu privasi dan keamanan publik. Operator *drone* diwajibkan untuk mematuhi aturan tersebut termasuk menghindari penerbangan di wilayah-wilayah pribadi tanpa izin. Pengawasan terhadap kepatuhan penggunaan *drone* dilakukan oleh otoritas penerbangan sipil, yang memiliki wewenang untuk memberikan sanksi kepada *operator* yang melanggar.

Korban penyalahgunaan *drone* memiliki akses dalam mekanisme penegakan hukum lainnya. Korban dapat melaporkan insiden kepada pihak berwenang seperti kepolisian atau badan pengawas komunikasi dan informasi. Laporan yang dibuat akan memicu investigasi resmi yang bertujuan untuk mengidentifikasi dan menuntut pelaku. Korban berhak mendapatkan perlindungan dari ancaman dan intimidasi, serta dukungan dalam bentuk bantuan hukum dan psikologis selama mekanisme ini berlangsung. Mekanisme tersebut memastikan bahwa hak-hak korban terlindungi dan mereka mendapatkan keadilan yang layak.

Korban juga dapat mencari keadilan melalui jalur perdata dengan mengajukan gugatan terhadap pelaku. Gugatan perdata memungkinkan korban untuk menuntut ganti rugi atas kerugian materiil dan immateriil yang dialami akibat pelanggaran privasi. Pengadilan memiliki wewenang untuk memerintahkan pelaku untuk menghentikan penyebaran konten ilegal dan memberikan kompensasi

finansial kepada korban. Langkah tersebut tidak hanya membantu korban pulih dari kerugian yang dialami tetapi juga menegaskan pentingnya perlindungan privasi dalam era teknologi yang semakin maju. Kombinasi perlindungan hukum yang komprehensif dan mekanisme penegakan hukum yang efektif akan membuat masyarakat merasa lebih aman dan terlindungi dari ancaman penyalahgunaan teknologi *drone*.

2) Pendekatan sosial

Pendekatan sosial bertujuan menciptakan budaya yang menghargai hukum dan etika, serta meningkatkan partisipasi masyarakat dalam menjaga keamanan dan ketertiban. Pendekatan sosial berfokus pada peningkatan kesadaran masyarakat terhadap pentingnya mematuhi peraturan dan etika dalam penggunaan teknologi, termasuk *drone*. Melalui penyuluhan dan kampanye edukatif, seperti kampanye *Know Before U Fly (KB4UFLY)* di Amerika Serikat, masyarakat dapat diberi pemahaman mengenai manfaat dan risiko dari penggunaan *drone*, serta pentingnya menjaga privasi dan keamanan orang lain. Kampanye tersebut tidak hanya menyasar pengguna teknologi, tetapi juga masyarakat umum agar dapat mengenali dan melaporkan potensi penyalahgunaan yang terjadi.[27]

3) Pendekatan teknologi

Pendekatan teknologi berperan penting dalam mendukung perlindungan hukum preventif dengan menyediakan alat dan sistem yang dapat membantu mencegah pelanggaran hukum. Misalnya, teknologi *geo-fencing* dapat digunakan untuk membatasi area penerbangan *drone* agar tidak memasuki zona terlarang.[28] Teknologi pengawasan yang canggih dapat digunakan untuk memantau aktivitas *drone* secara *real-time* dan mendeteksi aktivitas yang mencurigakan. Pengembangan teknologi keamanan yang dapat mengenali dan merespons ancaman secara otomatis juga dapat menjadi alat yang efektif dalam mencegah pelanggaran hukum. Berdasarkan hal tersebut maka perlindungan hukum preventif dapat dilakukan dengan lebih efisien dan efektif melalui pemanfaatan kemajuan teknologi.

Perlindungan hukum preventif dapat dijalankan secara lebih komprehensif dan berkelanjutan dengan menggabungkan pendekatan hukum, sosial, dan teknologi. Ketiga pendekatan yang digunakan akan saling melengkapi dan memperkuat, sehingga dapat menciptakan sistem yang mampu mencegah pelanggaran hukum secara efektif. Pendekatan hukum menyediakan kerangka peraturan yang jelas, pendekatan sosial meningkatkan kesadaran dan partisipasi masyarakat, sementara pendekatan teknologi memberikan alat untuk pengawasan dan pencegahan. Kolaborasi antara ketiga pendekatan dapat menciptakan lingkungan yang lebih aman dan tertib, serta mencegah terjadinya pelanggaran hukum.

IV. Simpulan

Berdasarkan hasil analisa dan pembahasan maka perlindungan hukum korban terhadap pelanggaran hak privasi dalam pembuatan konten menggunakan *drone* menunjukkan bahwa pelanggaran privasi oleh *drone* sering kali didasari oleh keyakinan pelaku yang merasa berhak mengawasi seseorang atau tidak peduli dengan dampak dari tindakannya. Bentuk-bentuk pelanggaran privasi meliputi pengawasan tidak sah, pengintaian, penyusupan, dan penggunaan untuk kejahatan. Perlindungan hukum terhadap korban dapat dilakukan melalui pendekatan hukum represif dan preventif. Pendekatan represif berfokus pada penjatuhan sanksi pidana bagi pelaku, sedangkan pendekatan preventif mengatur batasan-batasan tindakan dan mengedukasi masyarakat. Akhirnya perlindungan hukum terhadap korban pelanggaran hak privasi dalam pembuatan konten menggunakan *drone* dapat tercapai secara efektif dan efisien melalui gabungan pendekatan hukum, sosial, dan teknologi. Pencegahan secara pribadi dapat dilakukan oleh setiap orang dengan mengkonfrontasi *pilot drone* dan melaporkannya ke pihak berwenang jika terjadi pelanggaran demi mewujudkan lingkungan yang lebih aman, nyaman, tertib dan saling menghargai hak privasi sebagai bagian pemenuhan dan perlindungan hak asasi manusia untuk mencegah terjadinya pelanggaran hukum.

Daftar Pustaka.

Alfian, M. (2018). Penguatan Hukum Cyber Crime Di Indonesia Dalam Perspektif Peraturan Perundang-Undangan. *Kosmik Hukum, 17*(2).

Bassi, E. (2019). European Drones Regulation: Today's Legal Challenges. *2019 International Conference on*

[27] Know Before You Fly. (2023). Recreational Users. Diakses pada 10 Juni 2024, https://knowbeforeyoufly.org/home.
[28] Hermand, E., et al. Constrained Control of UAVs in Geofencing Applications. *26th Mediterranean Conference on Control and Automation (Med),* IEEE, pp 217–22. Hlm.219.

Unmanned Aircraft Systems (ICUAS), IEEE, 443–50.

Birnbach, S., Baker, R., & Martinovic, I. (2017). Wi-Fly?: Detecting Privacy Invasion Attacks by Consumer Drones. *NDSS*.

Boštjan, S. (2016). Drones in (Slovene) Criminal Investigation. *Kriminalistička Teorija i Praksa*, *3(*2), 7–25.

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Technology and Economics Law Journal, 2*(2), 3.

Choi, Y. J. (2022). Security Threat Scenarios of Drones and Anti-Drone Technology. *Academy of Strategic Management Journal, 21*(1), 1–7.

Hermand, E., et al. Constrained Control of UAVs in Geofencing Applications. *26th Mediterranean Conference on Control and Automation (Med),* IEEE, pp 217–22.

Husna, S. K. I., & Najicha, F. U. (2023). Pancasila Dan Hubungannya Dengan Hak Asasi Manusia Di Indonesia. *Civic Education: Media Kajian Pancasila Dan Kewarganegaraan, 7*(2), 104–12.

Khan, M. A., et al. (2022). On the Detection of Unauthorized Drones—Techniques and Future Perspectives: A Review. *IEEE Sensors Journal, 22*(2), 11439–55.

Kunertova, D. (2023). The War in Ukraine Shows the Game-Changing Effect of Drones Depends on the Game. *Bulletin of the Atomic Scientists, 79*(2), 95–102.

Marufah, N., Rahmat, H.K., & Widana, D. K. K. I. (2020). Degradasi Moral Sebagai Dampak Kejahatan Siber Pada Generasi Millenial Di Indonesia. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial, 7*(1), 191–201.

Ningsih, C. S., et al. (2021). Hak Kebebasan Berpendapat Yang Semakin Menyempit Dan Memburuk. *Jurnal Syntax Fusion, 1*(2), 25–39.

Prastyanti, Rina Arum. "Perlindungan Keamanan Siber Berdasarkan Perspektif Hak Asasi Manusia." In *Prosiding Seminar Nasional Hukum, Bisnis, Sains Dan Teknologi*, 1:275, 2020.

Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *Jatiswara, 34*(3), 239–249.

Ramadhan, M. A., & Fikri, R. (2024). Penggunaan Drone dalam Kejahatan: Tinjauan Terhadap Penggunaan Teknologi UAV untuk Pencurian Data dan Serangan Fisik. *Jurnal Media Akademik (JMA), 2*(6).

Rugo, A., Ardagna, C. A., & Ioini, N. E. (2022). A Security Review in the UAVNet Era: Threats, Countermeasures, and Gap Analysis. *ACM Computing Surveys (CSUR), 55*(1), 1–35.

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik. *Jurnal Ham, 11*(2), 285–99.

Sarjito, A., & Lelyana, N. (2023). Analisis Dampak Persepsi Ancaman Drone Terhadap Pembuatan Kebijakan Pertahanan Dan Proses Alokasi Sumber Daya. *Jurnal of Management and Social Sciences, 1*(4), 14–32.

Saroinsong, H. S., Poekoel, V. C., & Manembu, P. D. (2018). Rancang Bangun Wahana Pesawat Tanpa Awak (Fixed Wing) Berbasis Ardupilot. *Jurnal Teknik Elektro Dan Komputer, 7*(1), 73–84.

Sinaga, A. Br., Usman, U., & Wahyudhi, D. (2021). Perbuatan Menguntit (Stalking) Dalam Perspektif Kebijakan Hukum Pidana Indonesia. *PAMPAS: Journal of Criminal Law, 2*(2), 15–28

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 1 Tahun 2024 tentang Informasi Teknologi dan Elektronik

Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia

Permenhub Nomor 63 tahun 2021 tentang Peraturan Keselamatan Penerbangan Sipil Bagian 107

Permenhub Nomor 37 Tahun 2020 tentang Pengoperasian Pesawat Udara Tanpa Awak Di Ruang Udara Yang Dilayani Indonesia

Algar, J. (2014). DARPA Wants Drones to Be Swift as Hawks, Small as Insects. Diakses pada 30 Desember

2023, https://www.techtimes.com/articles/23876/20141230/darpa-wants-drones-to-be-swift-as-hawks-small-as-insects.htm.

Bev, G. (2023). I'm Being Watched: How to Deal With Stalkers and Spies. Diakses pada 15 Desember 2023, https://owlcation.com/social-sciences/Somebody-is-Watching-Me.

Crawford, J. (2018). 10 Crimes Committed Using A Drone. Diakses pada 30 Desember 2023, https://listverse.com/2018/07/26/10-crimes-committed-using-a-drone/.

Dian, R. (2023). Ibu Hamil Yang Direkam Tanpa Izin Alami Keguguran Saat Turun Dari KRL. Diakses pada 20 Desember 2023, https://narasi.tv/read/narasi-daily/viral-ibu-hamil-direkam-tanpa-izin-di-krl.

Hakim, D. (2022). Outlook Industri Drone Indonesia 2023. Diakses pada 20 Mei 2024, https://astta.id/2022/11/24/outlook-industri-drone-indonesia-2023/.

Know Before You Fly. (2023). Recreational Users. Diakses pada 10 Juni 2024, https://knowbeforeyoufly.org/home.